MARK J. BOURASSA, ESQ.
Nevada Bar No. 7999
JENNIFER A. FORNETTI, ESQ.
Nevada Bar No 7644
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., #100
Las Vegas, Nevada 89102
Tel: (702) 851-2180
Fax: (702) 851-2189
Email: mbourassa@blgwins.com
jfornetti@blgwins.com
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

BRYAN KHALILIRAD, on behalf of himself and all others similarly situated, Plaintiff, v. **MGM RESORTS INTERNATIONAL,** Defendant.	**Case No.:** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Bryan Khalilirad ("Plaintiff"), on behalf of himself and all others similarly situated, brings this class action lawsuit against MGM Resorts International ("MGM" or "Defendant"), and alleges based upon personal information and belief and the investigation of his counsel as follows:

INTRODUCTION

1. Bryan Khalilirad, individually and on behalf of all others similarly situated, brings this class action on behalf of persons who have suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Defendant's egregious failure to safeguard their customers' highly sensitive personally identifiable information ("PII"), including, but not limited to, names, mailing addresses, phone numbers, and other personal data.

2. Specifically, "[o]n or about July 7, 2019, an individual accessed MGM Resorts International's computer network system without permission. The individual downloaded partial

customer data from MGM's computer systems, then posted and disclosed part of the data on a closed internet forum" (the "MGM Data Breach").

3. Despite the fact that the threat of a data breach has been a well-known risk to Defendant, Defendant failed to take reasonable steps to adequately protect the ultra-sensitive, highly sought after PII of more than 200 million MGM customers. Plaintiff and the Class are now left to deal with the direct consequences of Defendant's failures.

4. The data breach was the inevitable result of Defendant's lax approach to the security of consumers' PII, an approach characterized by neglect, incompetence, and an overarching desire to minimize costs.

5. Defendant's actions have left MGM customers' PII exposed and accessible to hackers. Consequently, Plaintiff and the Class have incurred, and will continue to incur, significant damages in taking protective measures to reduce risk of identity theft and other fraudulent activity, among other things.

6. Plaintiff seeks to recover the costs that he and others similarly situated have been forced to bear as a direct result of Defendant's data breach and to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this breach.

PARTIES

7. Plaintiff Bryan Khalilirad is a citizen of the State of California. During the Class Period, Plaintiff has been a member of MGM's M life Rewards program for approximately three years and has provided MGM his PII. Further, he has made hotel reservations and stayed at MGM properties approximately three times since 2017 and has also used MGM's online gaming service. As a result of Defendant's actions, Plaintiff will be subject to a substantial risk for identify theft due to Defendant's data breach.

8. Defendant MGM Resorts International is a publicly traded corporation with a principal place of business at 3600 Las Vegas Blvd, South Las Vegas, NV 89109. MGM is a citizen of Delaware and Nevada.

/ / /

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 putative class members (defined below); and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendant.

10. This Court has personal jurisdiction over Defendant MGM as it maintains its principal headquarters in Nevada, is registered to conduct business in Nevada, regularly conducts business in Nevada, and has sufficient minimum contacts in Nevada. Defendant intentionally avails itself of this jurisdiction by conducting MGM's corporate operations here and promoting, selling, and marketing MGM's services to resident Nevada consumers and entities.

11. Venue is proper in this District under 28 U.S.C. §1391(a) because MGM's principal place of business is in Nevada and a substantial part of the events, acts, and omissions giving rise to the claims of the Plaintiff occurred in this District.

FACTUAL ALLEGATIONS

Background

12. Founded in 1986 as MGM Grand, Inc., MGM today "is an S&P 500® global entertainment company with national and international locations featuring best-in-class hotels and casinos, state-of-the-art meetings and conference spaces, incredible live and theatrical entertainment experiences, and an extensive array of restaurant, nightlife and retail offerings."[1]

13. During the Class Period, MGM collected PII directly and indirectly from consumers and collected and maintained a substantial and diverse amount of PII.[2]

---

[1] MGM, About MGM Resorts, https://www.mgmresorts.com/en/company.html (last accessed April 23, 2020).

[2] MGM, Privacy Policy, https://www.mgmresorts.com/en/privacy-policy.html ("A. Personal Information. When you visit, use, and/or access MGM Resorts or MGM Online Services, you may provide us with (and/or we may collect) information by which you can be personally identified including your name, date of birth, postal address, e-mail address, and telephone number, and videos, recordings, and images of you ("Personal Information"). We may also obtain Personal Information from third parties.") (last accessed April 23, 2020).

Plaintiff and the Class Relied on MGM to Adequately Protect Their Sensitive Information

14. Defendant has a well-established and clear legal duty to act reasonably to protect PII they collect and possess from exposure to unauthorized third parties.

15. When Plaintiff and the Class provided Defendant with their most sensitive information, or when Defendant received such information in some other manner, Plaintiff and the Class reasonably expected that such information would be stored by Defendant in a safe and confidential manner, using all reasonable safeguards and protections.

The MGM Data Breach

16. On or about September 5, 2019, MGM notified affected customers and various governmental agencies that "[o]n or about July 7, 2019, an individual accessed MGM Resorts International's computer network system without permission. The individual downloaded partial customer data from MGM's computer systems, then posted and disclosed part of the data on a closed internet forum."

17. Publicly available information indicates more than 200 million MGM customers may have had their PII compromised in the MGM Data Breach. As recently as February 19, 2020, ZDNet revealed that the PII of more than 10.6 million MGM hotel guests had been posted to a popular internet hacking forum.

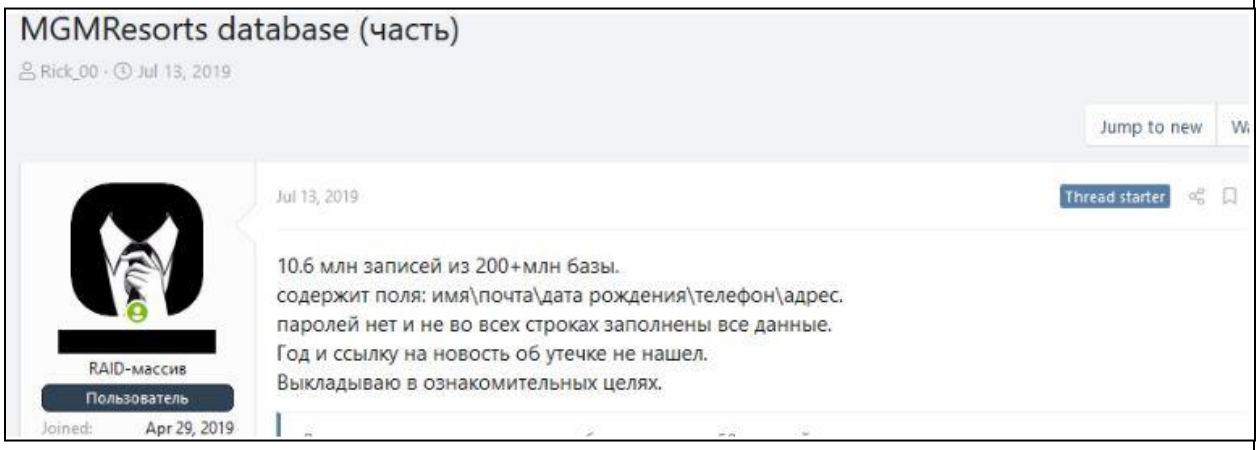
18. The information obtained by the hackers includes the affected individuals' first and last names, home addresses, telephone numbers, and other personal data.

19. According to the cybersecurity firm KELA, the hackers were distributing the PII in hacking forums by at least July 13, 2019.[3]

20. Below is a screenshot of one post, written in Russian and identifying MGM by name, listing the stolen information.

---

[3] See Catalin Cimpanu, ZDNet, Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum (Feb. 19, 2020), https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/ (last accessed April 23, 2020).



In English, the post reads:

> 10.6 million records out of a database of 200+million.
>
> Contains fields: name\e-mail\birthdate\telephone\address.
>
> No passwords and not all lines are filled with all data.
>
> Year and link reference to news about the leak not found.
>
> I am spreading for informational purposes.

21. According to ZDNet, the above "data dump" contains the PII of 10,683,188 MGM customers. Below is a screenshot of the file containing the stolen information.

22. Another leading cybersecurity expert confirmed the MGM Data Breach compromised 3,081,321 unique email addresses stemming back to 2017.[4]

23. Despite hackers identifying it by name as early as July 13, 2019, MGM claims it did not determine which customers were affected until August 9, 2019.

24. Then, once making this determination, MGM waited until at least August 22, 2019, to notify the customers whose Personally Identifiable Information was compromised in the MGM Data Breach.[5]

25. To date, MGM has not explained why it took more than a month to discover and determine what information was compromised or why it took another two weeks after that determination to notify its affected customers.

26. The breadth of data compromised in the MGM Data Breach makes the information particularly valuable to thieves and leaves MGM's customers especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

Plaintiff and the Class Have Been, Are Currently Being, and Will Be Harmed by the Data Breach

27. Plaintiff is a member of MGM's M life Rewards program. MGM launched the M life Rewards program on January 11, 2011 to "allow[ ] members to not only accumulate rewards on gambling, but also their total resort stay."[6]

28. Since at least October 2, 2017, MGM's website has disclosed that "[b]y enrolling in the M life Rewards Program and/or using your Card, members consent to the terms of the MGM Privacy Policy and the sharing of their personal information among all casinos, resorts,

---

[4] HIBP, Troy Hunt, Pwned websites, https://haveibeenpwned.com/PwnedWebsites#MindJolt (last accessed April 23, 2020).

[5] Vegas Message Board, Data breach at MGM Resorts in July 2019?, https://www.vegasmessageboard.com/forums/index.php?threads/data-breach-at-mgm-resorts-in-july-2019.165346/ (last accessed April 23, 2020).

[6] Amanda Finnegan, Las Vegas Sun, MGM Resorts launches M Life rewards program, will track nongaming spending, https://lasvegassun.com/news/2011/jan/11/mgm-resorts-launches-m-life-rewards-program-will-t/ (last accessed April 23, 2020).

and properties of MGM Resorts International.[7] At that time, MGM's August 7, 2017 Privacy Policy defined Personal to include customers' " name, date of birth, postal address, e-mail address, and telephone number, and videos, recordings, and images of you."[8] The August 7, 2017 Privacy Policy further disclosed that MGM might also collect "information about the vehicle you park including an image of the vehicle, the vehicle's make, model, and license plate number[,]" "information about your purchases, reservations, and gaming activity," "credit or debit card number, financial account number, biometrics, driver's license number, government-issued identification card number, social security number, passport number, or naturalization number[,]" among other information.[9]

29. MGM collects even more information about its customers and M life Reward program members today, including their "name, e-mail address, postal mail address, telephone number, date of birth, credit card number, passport number, driver's license number, bank account number, social security number; legally protected characteristics including gender, race, and sexual orientation; commercial information including your gaming, entertainment, travel, dining, lodging, and business transactions; audio, visual, and biometric-related information including facial recognition information; professional or employment information."[10]

30. Plaintiff is aware of providing at least the following information to MGM as part of his membership in MGM's M life Rewards program: first name, last name, email address, password, telephone number, date of birth, home address, and security question answer. In turn,

---

[7] Internet Archive Wayback Machine, MGM Resorts M life Rewards, https://web.archive.org/web/20171002095927/https://www.mgmresorts.com/en/mlife-rewards-program/program-rules.html (archived on Oct. 2, 2017) (last accessed April 23, 2020).

[8] Internet Archive Wayback Machine, MGM Resorts Privacy Policy, https://web.archive.org/web/20170927220503/https://www.mgmresorts.com/en/privacy-policy.html (archived on Sept. 10, 2017) (last accessed Feb. 27, 2020).

[9] *Id*.

[10] MGM, Privacy Policy, https://www.mgmresorts.com/en/privacy-policy.html (effective Jan. 1, 2020) (last accessed April 23, 2020).

when Plaintiff made reservations at MGM locations, he would sign into his M life Rewards program account, which would populate the reservation fields with his Personal Information.

31. According to MGM's notice of the MGM Data Breach, at minimum, Plaintiff's "First Name, Last Name, and Driver's License Number" were compromised in the MGM Data Breach.

32. The data breach has inflicted immediate, hard costs on Plaintiff and members of the Class.

33. Defendant failed to follow industry standards and failed to effectively monitor their security systems to ensure the safety of customer information. Defendant's substandard security protocols and failure to adequately monitor for unauthorized intrusion caused Plaintiff and the Class's PII to be compromised for years without detection by Defendant.

34. Plaintiff and the Class have incurred, and will continue to incur, substantial damage because of Defendant's failures to meet reasonable standards of data security.

35. As a result of the Defendant's data breach, Plaintiff and the Class are required to cancel payment cards, change or close accounts, investigate fraudulent activity, and take other steps to protect themselves in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent transactions.

36. Sensitive personal and financial information, like the information compromised in this breach, is extremely valuable. Criminals have gained access to complete profiles of individuals' personal and financial information. They can now use this data to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. In this manner, unauthorized third parties can assume the stolen identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return. A report by the

Department of Justice found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information.[11]

37. Consequently, had consumers known the truth about MGM's data security practices—that they did not adequately protect and store their data—they would not have stayed at an MGM property, purchased products or services at an MGM property, and/or would have paid less. As such, Plaintiff and Class members did not receive the benefit of their bargain with MGM because they paid for the value of services they expected but did not receive.

38. MGM itself acknowledged the harm caused by its MGM Data Breach because it offered affected customers complimentary "12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services" as a result of the MGM Data Breach. However, such services are woefully inadequate to protect Plaintiff and the Class members from a virtual lifetime of identity theft risk and does nothing to reimburse Plaintiff and the Class members from the injuries they have already suffered. Indeed, such services may do nothing to protect from common uses of PII by hackers such as potential fraud, tax fraud, or fraudulent business or payday loans, for instance.

39. Ultimately, Plaintiff and the Class are faced with considerable present injury, and an immediate future of continually unfolding new and continued injures as a result of Defendant's avoidable data breach.

Defendant Knew that a Breach of Their Compute Systems Was a Foreseeable Risk

40. With data breaches and identity theft on the rise, Defendant undoubtedly knew that a breach of their computer systems was a foreseeable risk. They also knew what the repercussions of such a breach would be.

41. PII have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell such stolen data as a result of the "proliferation of open and

[11] Erika Harrell, Victims of Identity Theft, 2014, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 (Sept. 2015) at 1, https://www.bjs.gov/content/pub/pdf/ vit14.pdf.

anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[12]

42. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center ("ITRC"), in 2017, there were 1,579 reported data breaches in the United States, an all-time high.[13] More than 178.93 million records reportedly were exposed in those breaches.[14] The IRTC reported that approximately 60% of the data breaches were the result of hacking.[15]

43. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2017, affecting approximately 16.7 million victims in the U.S., with the amount stolen rising to $16.8 billion.[16]

44. Following several high-profile data breaches in recent years, including those involving Target, Experian, Yahoo, Home Depot, Sony, and Marriott, Defendant was on notice of the very real risk that hackers could exploit vulnerabilities in Defendant's data security.

45. Thus, Defendant knew, given the vast amount of PII they managed, that they were a target of attempted cyber and other security threats and therefore understood the risks posed by their insecure and vulnerable computer systems and website. They also understood the need to safeguard PII and the impact a data breach would have on their customers, including Plaintiff and the Class.

---

[12] Brian Krebs, The Value of a Hacked Company, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[13] Data Breach Reports: 2017 End of Year Report, IDENTITY THEFT RESOURCE CENTER, at 6 (2018), http://www.idtheftcenter.org/images/breach/2017/DataBreachReport_2017.pdf.

[14] *Id*.

[15] *Id*. at 4.

[16] Javelin Strategy & Research, Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-usvictims-2017-according-new-javelin.

Defendant Failed to Comply with Federal Trade Commission Requirements

46. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. §45.

47. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

48. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

49. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

50. In the months and years leading up to the data breach and during the course of the breach itself, Defendant failed to follow the guidelines recommended by the FTC. Further, by failing to have reasonable data security measures in place, Defendant engaged in unfair acts or practices within the meaning of Section 5 of the FTC Act.

CLASS ACTION ALLEGATIONS

51. Plaintiff brings this action on behalf of himself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following nationwide class and subclass (collectively, the "Class"):

Nationwide Class: All persons in the United States whose PII was accessed, copied, stolen, or compromised by an unauthorized party as a result of the MGM Data Breach.

California Subclass: All persons in California whose PII was accessed, copied, stolen, or compromised by an unauthorized party as a result of the MGM Data Breach.

52. Excluded from the Class are MGM and its officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

Rule 23(a)

53. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

54. **Numerosity**. The members of the Class are so numerous that joinder would be impracticable. Plaintiff believes the number of Class members exceeds one million.

55. **Commonality**. There are common questions of law and fact that predominate over questions affecting only individual Class members. These common legal and factual questions include, but are not limited to:

a. whether Defendant owed a duty to Plaintiff and members of the Class to protect PII;

b. whether Defendant failed to provide reasonable security to protect PII;

c. whether Defendant negligently or otherwise improperly allowed PII to be accessed by third parties;

d. whether Defendant failed to adequately notify Plaintiff and members of the Class that their data systems were breached;

e. whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses;

f. whether Defendant's actions, which failed to reasonably secure Plaintiff's and the Class's PII, proximately caused the injuries suffered by Plaintiff and members of the Class;

g. whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. whether Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

56. **Typicality**. Plaintiff's claims are typical of the claims of the absent class members and have a common origin and basis. Plaintiff and Class members are all persons and entities injured by Defendant's data breach. Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories, namely, the Defendant's data breach. If prosecuted individually, the claims of each Class member would necessarily rely upon the same material facts and legal theories and seek the same relief.

57. **Adequacy**. Plaintiff will fully and adequately assert and protect the interests of the absent Class members and has retained Class counsel who have considerable experience in class action litigation concerning corporate data security and the resources necessary to prosecute this case. Neither Plaintiff nor his attorneys have any interests contrary to or conflicting with the interests of absent class members.

Rule 23(b)(3)

58. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

59. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class members to litigate their claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

60. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

COUNT I
NEGLIGENCE
(Brought by Plaintiff and the Nationwide Class)

61. Plaintiff incorporates by reference all of the above allegations as if fully set forth herein.

62. Defendant owed Plaintiff and the Class a common-law duty to exercise reasonable care in the collection and storage of their PII.

63. Defendant's duty included an obligation to take reasonable protective measures against the foreseeable risk to Plaintiff and the Class that harm would inevitably result if their PII was interfered with, stolen, or copied while in Defendant's possession.

64. Defendant knew or should have known that by collecting and storing PII, they created a valuable trove of information that was a foreseeable target for third-party interference, copying, or theft.

65. Defendant knew or should have known that companies possessing similar data troves have in fact been targeted for hacking in highly publicized data breaches, including Yahoo, Equifax, Wyndham, Home Depot, Sony, and Marriott, to name just a few.

66. Once Defendant chose to collect and store PII belonging to Plaintiff and the Class, only Defendant was in a position to secure their valuable data trove from the foreseeable risk of third-party interference, copying, or theft.

67. Defendant's duty to act reasonably in collecting and storing PII also arises under Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII.

68. Plaintiff and the Class reasonably assumed that a major corporation like Defendant would adhere to basic industry standards with respect to the collection and storage of PII.

69. Defendant breached its common law and statutory duties by failing to use reasonable data collection, storage, and security practices. In addition to Defendant's initial

negligence in storing PII on a system vulnerable to outside penetration, Defendant's negligence likely persisted for years, during which Defendant failed to detect the ongoing compromise and failed to improve security practices in a way that could end the breach. During those years, Defendant missed numerous opportunities to stop or mitigate the data breach at a point in time when fewer individuals might have been harmed.

70. Defendant's negligent data collection and storage practices led to a foreseeable result: the valuable PII associated with Plaintiff and the Class was copied or stolen by unauthorized third parties, who are now well-equipped to perpetrate fraud and identity theft at the expense of Plaintiff and the Class.

71. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have been harmed in several ways. They are all now at an increased risk of being victims of identity theft, financial impersonation, and a variety of other fraudulent schemes, including those that use targeted phishing or social engineering techniques facilitated by the using of compromised PII elements against victims. To guard against the heightened risk of these crimes, Plaintiff and the Class will need to invest more of their time and money on monitoring their finances, tax records, credit scores, and accounts of all types, including financial institution, social media, loyalty programs, online retailers, and others.

72. Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, investing time and money in cancelling payment cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

73. But for Defendant's negligence, the PII of Plaintiff and the Class would not have been exposed, or in the alternative, Plaintiff and the Class would have at least learned of the compromise at an earlier point in time when some of their damages may have been mitigated.

/ / /

/ / /

/ / /

/ / /

/ / /

COUNT II
NEGLIGENCE *PER SE*
(Brought by Plaintiff and the Nationwide Class)

74. Plaintiff incorporates by reference all of the above allegations as if fully set forth herein.

75. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty.

76. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, the length of time the information was maintained on an apparently vulnerable system, and the foreseeable consequences of a data breach at a major, international hospitality company, including, specifically, the immense damages that would result to consumers.

77. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

78. Plaintiff and members of the Class are consumers and are within the class of persons that Section 5 of the FTC Act was intended to protect.

79. The harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

80. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injury, including, but not limited to, investing time and money in cancelling payment cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

/ / /

/ / /

COUNT III
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §17200, *et seq*.
(Brought by Plaintiff and the California Subclass)

81. Plaintiff incorporates by reference all of the above allegations as if fully set forth herein.

82. Defendant violated the California Business & Professions Code §17200 *et seq*. by engaging in unlawful, unfair, or fraudulent practices.

83. Plaintiff, Class members, and Defendant all are "persons" as defined by Cal. Bus. & Prof. Code §17201.

84. Defendant's violation of Section 5 of the FTC Act was an unlawful, unfair, or fraudulent practice under Cal. Bus. & Prof. Code §17200.

85. As described above, Defendant negligently and recklessly failed to use reasonable care in collecting and storing the PII associated with Plaintiff and the Class.

86. Defendant did not disclose the compromised state of its data systems, despite regularly and repeatedly offering services to, transacting with, and collecting PII from Plaintiff and the Class.

87. If Plaintiff and the Class members had known that Defendant was not investing in or utilizing reasonable security practices, or that Defendant's PII storage systems were compromised, Plaintiff and Class members would have spent less on Defendant's services or would not have used Defendant's services at all.

88. By failing to invest in reasonable security measures while at the same time failing to disclose that their data systems were compromised, Defendant was able reap an illegitimate financial benefit at the expense of Plaintiff and the Class.

89. Plaintiff and the Class seek relief under Cal. Bus. & Prof. Code §17200 *et seq*. including, but not limited to, restitution to Plaintiff and the Class of money or property that Defendant may have acquired by means of Defendant's unlawful or unfair practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair

business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

COUNT IV
DECLARATORY AND EQUITABLE RELIEF
(Brought by Plaintiff and the Nationwide Class)

90. Plaintiff incorporates by reference all of the above allegations as if fully set forth herein.

91. Under the Declaratory Judgment Act, 28 U.S.C. §2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

92. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure their customers' PII, specifically including information pertaining to PII used by Defendant's customers;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure their customers' PII; and

c. Defendant's ongoing breaches of their legal duty continue to cause Plaintiff and the Class harm.

93. The Court also should issue corresponding injunctive relief requiring Defendant to employ adequate security protocols, consistent with industry standards, to protect PII. Specifically, this injunction should, among other things, direct Defendant to:

a. utilize industry standard encryption to encrypt the transmission of cardholder data at all times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. engage third-party auditors, consistent with industry standards, to test systems for weakness and upgrade any such weakness found;

e. audit, test, and train data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test systems for security vulnerabilities, consistent with industry standards; and

g. install all upgrades recommended by manufacturers of security software and firewalls used by Defendant.

94. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's data occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

95. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to Defendant, if an injunction is issued. Among other things, if another massive data breach occurs with Defendant's data, Plaintiff and members of the Class will likely incur tens of millions of dollars in damages. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal and Defendant has a pre-existing legal obligation to employ such measures.

96. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another breach of Defendant's systems, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class and California Subclass and appoint Plaintiff and Plaintiff's counsel to represent the Classes;

B. Enter a monetary judgment in favor of Plaintiff and the Classes to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment as described herein;

D. Grant the injunctive relief requested herein;

E. Award Plaintiff and the Classes reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all claims so triable.

Date: April 24, 2020

Respectfully submitted,

/s/ Mark J. Bourassa

Mark J. Bourassa (NBN 7999)
Jennifer A. Fornetti (NBN 7644)
THE BOURASSA LAW GROUP
2350 W. Charleston Blvd., #100
Las Vegas, Nevada 89102
Tel: (702) 851-2180
Fax: (702) 851-2189
mbourassa@blgwins.com
jfornetti@blgwins.com

To be admitted pro hac vice:

Jonathan M. Jagher
Kimberly A. Justice
FREED KANNER LONDON & MILLEN LLC
923 Fayette Street
Conshohocken, PA 19428
Tel.: (610) 234-6487
Fax: (224) 632-4521
jjagher@fklmlaw.com
kjustice@fklmlaw.com

Douglas A. Millen
Michael E. Moskovitz
Brian M. Hogan
FREED KANNER LONDON & MILLEN LLC
2201 Waukegan Road, Suite 130
Bannockburn, IL 60015
Tel.: (224) 632-4500
Fax: (224) 632-4521
dmillen@fklmlaw.com
mmoskovitz@fklmlaw.com
bhogan@fklmlaw.com

Attorneys for Plaintiff and the Proposed Classes